

PRUEBA DE HABILIDADES CCNA

CLAUDIA PATRICIA NAVAS GUEVARA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
INGENIERIA DE SISTEMAS
PAMPLONA
2019**

CONTENIDO

| | |
|---|----|
| INTRODUCCIÓN..... | 4 |
| OBJETIVOS | 5 |
| 1. ESCENARIO 1..... | 6 |
| 1.1 TOPOLOGÍA DE RED | 6 |
| 1.2 ASIGNACIÓN DE DIRECCIONES IP | 6 |
| 1.3 CONFIGURACIÓN BÁSICA | 7 |
| 1.4 VERIFICAR LA TABLA DE ENRUTAMIENTO | 12 |
| 1.5 BALANCEO DE CARGA QUE PRESENTAN LOS ROUTERS | 14 |
| 1.6 DIAGNÓSTICO DE VECINOS USANDO EL COMANDO CDP | 15 |
| 1.7 PRUEBA DE CONECTIVIDAD USANDO EL COMANDO PING | 16 |
| 1.8 CONFIGURACIÓN DE ENRUTAMIENTO | 16 |
| 1.9 COMPROBAR LAS TABLAS DE ENRUTAMIENTO..... | 18 |
| 1.10 CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO | 20 |
| 1.11 COMPROBACIÓN DE LA RED INSTALADA | 21 |
| 1.12 TABLA DE CONDICIONES DE PRUEBA..... | 24 |
| 2. ESCENARIO 2..... | 27 |
| 2.1 CONFIGURACION BASICA | 27 |
| 2.2 ENRUTAMIENTO OSPF | 30 |
| 2.3 VLAN Y DHCP EQUIPOS DE BUCARAMANGA Y CUNDINAMARCA | 33 |
| 2.4 ALMACENAMIENTO EN SERVIDOR TFTP | 36 |
| 2.5 CONFIGURACIÓN DHCP EN ROUTER DE TUNJA | 39 |
| 2.6 LISTAS DE CONTROL DE ACCESO | 40 |
| 3. CONCLUSIONES | 43 |
| 4. REFERENCIAS BIBLIOGRÁFICAS | 44 |

RESUMEN

En este documento se aplican conceptos de configuración de redes en dos escenarios diferentes. Configuraciones básicas, enrutamiento a través de Vlans y listas de acceso forman parte de las aplicaciones trabajadas en cada uno. Servicios DHCP, enrutamiento OSPF, el cifrado de contraseñas o la implementación de un servidor TFTP como almacenamiento de archivos también son trabajadas.

ABSTRACT

In this document you will find the concepts of network configuration in two different scenarios. Basic configurations, routing through Vlans and access lists are part of the applications worked on each one. DHCP services, OSPF routing, password encryption or the implementation of a TFTP server as file storage are also worked.

INTRODUCCIÓN

Los avances tecnológicos y el interés de las empresas y el público en general por mejorar y prosperar, hace que el mundo de las redes y telecomunicaciones, igualmente crezcan y se expandan para ofrecer un portafolio de servicios que cumpla esos requerimientos.

Los casos que se presentan en este documento son un ejemplo de cómo se puede prestar un servicio integral dentro de una organización. Así mismo, se puede encontrar la configuración y enrutamiento de dos redes que ilustran al lector en lo que respecta a las configuraciones básicas de dispositivos y en configuraciones un poco más complejas.

El enrutamiento EIGRP, la asignación de direcciones IP a través del protocolo DHCP y la aplicación de listas de acceso, forman parte del trabajo recopilado en este documento.

OBJETIVOS

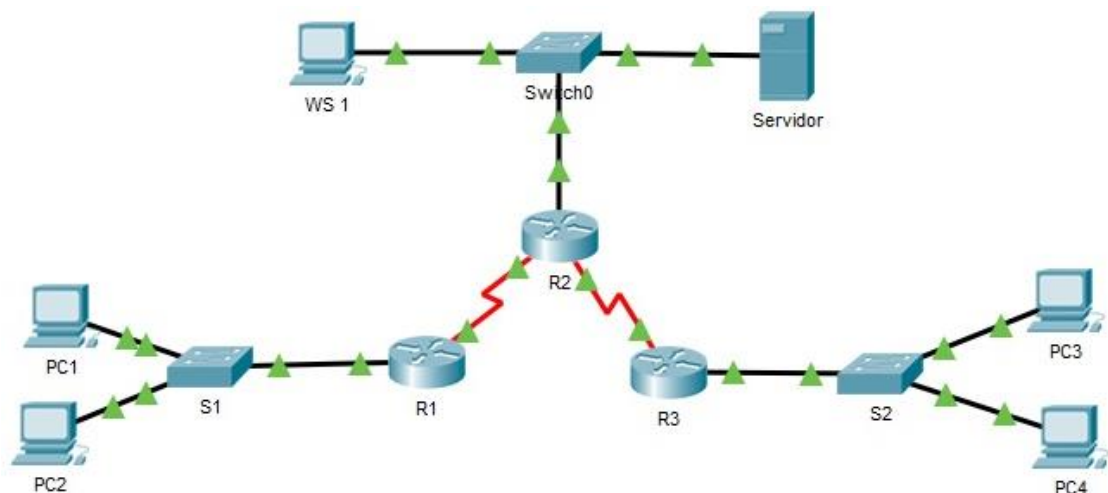
- Realizar la configuración básica en dispositivos como routers y switches para su puesta en funcionamiento.
- Implementar el enrutamiento OSPF en routers conectados por puertos seriales.
- Configurar las listas de acceso como mecanismo de seguridad dentro de una red.
- Implementar el servicio DHCP en un router para conocer su versatilidad y funcionamiento.

1. ESCENARIO 1.

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre si cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el lineamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

1.1 TOPOLOGÍA DE RED

Imagen 1. Topología de la red, escenario 1



1.2 ASIGNACIÓN DE DIRECCIONES IP

Se debe dividir la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

Se asigna la dirección 192.168.1.0 a la red.

A continuación, se muestra la tabla de direccionamiento para 8 subredes.

Tabla 1. División en subredes

| Número de subred | Dirección subred | Primera dirección de host utilizable | Ultima dirección de host utilizable | Dirección de Broadcast |
|------------------|------------------|--------------------------------------|-------------------------------------|------------------------|
| 0 | 192.168.1.0 | 192.168.1.1 | 192.168.1.30 | 192.168.1.31 |
| 1 | 192.168.1.32 | 192.168.1.33 | 192.168.1.62 | 192.168.1.63 |
| 2 | 192.168.1.64 | 192.168.1.65 | 192.168.1.94 | 192.168.1.95 |
| 3 | 192.168.1.96 | 192.168.1.97 | 192.168.1.126 | 192.168.1.127 |
| 4 | 192.168.1.128 | 192.168.1.129 | 192.168.1.158 | 192.168.1.159 |
| 5 | 192.168.1.160 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 |
| 6 | 192.168.1.192 | 192.168.1.193 | 192.168.1.222 | 192.168.1.223 |
| 7 | 192.168.1.224 | 192.168.1.225 | 192.168.1.254 | 192.168.1.255 |

1.3 CONFIGURACIÓN BÁSICA

Tabla 2. Configuración básica de los routers

| Nombre de Host | R1 | R2 | R3 |
|--|--------------|---------------|---------------|
| | MEDELLIN | BOGOTA | CALI |
| Dirección de IP en interfaz serial 0/0 | 192.168.1.99 | 192.168.1.98 | 192.168.1.131 |
| Dirección de IP en interfaz serial 0/1 | | 192.168.1.130 | |
| Dirección de IP en interfaz Fa0/0 | 192.168.1.33 | 192.168.1.1 | 192.168.1.65 |
| Protocolo de Enrutamiento | Eigrp | Eigrp | Eigrp |
| Sistema autónomo | 200 | 200 | 200 |
| Afirmaciones de red | 192.168.1.0 | 192.168.1.0 | 192.168.1.0 |

Para realizar la configuración básica, se utiliza el mismo procedimiento en los 3 routers:

R1 - MEDELLIN

Ingreso al modo de configuración global

```
Router>
```

```
Router>en
```

```
Router#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router (config) #
```

Asignación de un nombre al router

```
Router (config) # hostname MEDELLIN
```

```
MEDELLIN (config) #
```

Para evitar las búsquedas de DNS no deseada

```
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#
```

Para configurar un mensaje MOTD

```
MEDELLIN(config)#
MEDELLIN(config)#banner motd #
Enter TEXT message. End with the character '#'.
El acceso no autorizado esta prohibido. #
```

```
MEDELLIN(config)#
```

Asegurar el acceso (EXEC privilegiado y EXEC de usuario)

```
MEDELLIN(config)#
MEDELLIN(config)#enable secret class
MEDELLIN(config)#
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#
MEDELLIN(config)#
```

Configurar la encriptación de contraseñas

```
MEDELLIN(config)#
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN#
```

R2 – BOGOTA

Ingreso al modo de configuración global

```
Router>
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Asignación de un nombre al router

```
Router(config)# hostname BOGOTA
BOGOTA(config)#
```


Para evitar las búsquedas de DNS no deseada

```
BOGOTA(config)#  
BOGOTA(config)#no ip domain-lookup  
BOGOTA(config)#
```

Para configurar un mensaje MOTD

```
BOGOTA(config)#banner motd #  
Enter TEXT message. End with the character '#'.  
El acceso no autorizado esta prohibido!!.#
```

```
BOGOTA(config)#
```

Asegurar el acceso (EXEC privilegiado y EXEC de usuario)

```
BOGOTA(config)#  
BOGOTA(config)#enable secret class  
BOGOTA(config)#  
BOGOTA(config)#line console 0  
BOGOTA(config-line)#password cisco  
BOGOTA(config-line)#logging synchronous  
BOGOTA(config-line)#exit  
BOGOTA(config)#
```

Configurar la encriptación de contraseñas

```
BOGOTA(config)#  
BOGOTA(config)#service password-encryption  
BOGOTA(config)#  
BOGOTA(config)#exit  
BOGOTA#  
%SYS-5-CONFIG_I: Configured from console by console  
  
BOGOTA#
```

R3 – CALI

Ingreso al modo de configuración global

```
CALI>  
CALI>en  
CALI#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
CALI(config)#
```

Para evitar las búsquedas de DNS no deseada

```
CALI(config)#  
CALI(config)#no ip domain-lookup  
CALI(config)#
```

Para configurar un mensaje MOTD

```
CALI(config)#
CALI(config)#banner motd #
Enter TEXT message. End with the character '#'.
El acceso no autorizado esta prohibido!!! #

CALI(config)#
```

Asegurar el acceso (EXEC privilegiado y EXEC de usuario)

```
CALI(config)#
CALI(config)#enable secret class
CALI(config)#
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login synchronous
CALI(config-line)#exit
CALI(config)#
```

Configurar la encriptación de contraseñas

```
CALI(config)#
CALI(config)#service password-encryption
CALI(config)#
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console

CALI#
```

Se asignan las direcciones IP a las interfaces de acuerdo con la tabla de enrutamiento

R1 - MEDELLIN

```
MEDELLIN(config)#
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)# ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#clock rate 64000
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#exit
MEDELLIN(config)#
MEDELLIN(config)#int fa0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#exit
MEDELLIN(config)#
MEDELLIN(config)#
```

R2 - BOGOTA

```
BOGOTA(config)#
BOGOTA(config)#int S0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#
BOGOTA(config)#int S0/1/0
BOGOTA(config-if)#ip address 192.168.1.30 255.255.255.224
BOGOTA(config-if)#clock rate 64000
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#
BOGOTA(config)#int fa0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
```

R3 - CALI

```
CALI(config)#
CALI(config)#int s0/0/0
CALI(config-if)# ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#exit
CALI(config)#
CALI(config)#int fa0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#exit
CALI(config)#
CALI(config)#
```

Se asignan las IP a los PC

Red Medellin - PC1

Dirección ip: 192.168.1.35
Mascara: 255.255.255.0
Gateway: 192.168.1.33

Red Medellin – PC2

Dirección ip: 192.168.1.36
Mascara: 255.255.255.0
Gateway: 192.168.1.33

Red Cali – PC3

Dirección ip: 192.168.1.67
Mascara: 255.255.255.0
Gateway: 192.168.1.65

Red Cali – PC4

Dirección ip: 192.168.1.68
Mascara: 255.255.255.0
Gateway: 192.168.1.65

Red Bogotá – WS 1

Dirección ip: 192.168.1.5
Mascara: 255.255.255.0
Gateway: 192.168.1.1

Red Bogotá – Servidor

Dirección ip: 192.168.1.10
Mascara: 255.255.255.0
Gateway: 192.168.1.1

1.4 VERIFICAR LA TABLA DE ENRUTAMIENTO

Para comprobar las redes y sus rutas se verifica la tabla de enrutamiento en cada uno de los routers.

Se aplica el comando `show ip route` y se puede apreciar en cada router su configuración EIGRP

```

MEDELLIN#
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

```

Gateway of last resort is not set

```

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.98, 00:10:26, Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/21026560] via 192.168.1.98, 00:10:26, Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/21024000] via 192.168.1.98, 00:10:26, Serial0/0/0

```

MEDELLIN#

```

BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

```

Gateway of last resort is not set

```

    192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/20514560] via 192.168.1.99, 00:26:48, Serial0/0/0
D       192.168.1.64 [90/20514560] via 192.168.1.131, 00:26:48, Serial0/1/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/1/0

```

BOGOTA#

```

CALI#
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.130, 00:29:57, Serial0/0/0
D       192.168.1.32 [90/21026560] via 192.168.1.130, 00:29:57, Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/21024000] via 192.168.1.130, 00:29:57, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI#

```

1.5 BALANCEO DE CARGA QUE PRESENTAN LOS ROUTERS

Las plataformas que usan IOS tienen un máximo de 4 ECMP configurado por defecto, lo cual podemos ver cuando ingresa el comando **show ip protocols** en cada uno de los routers.

Imagen 2. ECMP configurado en R1, R2 y R3

```

MEDELLIN#
MEDELLIN#show ip protocols

Routing Protocol is "eigrp 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 200
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.1.32/27
    192.168.1.96/27
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.98     90            94897977
  Distance: internal 90 external 170

MEDELLIN#

BOGOTAS#
BOGOTAS#show ip protocols

Routing Protocol is "eigrp 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 200
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.1.96/27
    192.168.1.128/27
    192.168.1.0/27
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.131    90            94897977
    192.168.1.99     90            94897412
  Distance: internal 90 external 170

BOGOTAS#

CALI#
CALI#show ip protocols

Routing Protocol is "eigrp 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 200
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.128/27
    192.168.1.64/27
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.130    90            94897977
  Distance: internal 90 external 170

CALI#

```

1.6 DIAGNÓSTICO DE VECINOS USANDO EL COMANDO CDP

El router R1 (Medellín) está conectado al Sw1 por el puerto Fa0/0 y a su vez, el Sw1 está conectado al R1 por el puerto Fa0/1. Por otra parte, R1 está conectado al R2 (Bogotá) por el puerto s0/0/0 y Bogotá está conectada a Medellín por el puerto s0/0/0

```
MEDELLIN#
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
Sw1               Fas 0/0         167      S           2960      Fas 0/1
BOGOTA            Ser 0/0/0       173      R           C2800     Ser 0/0/0
MEDELLIN#
```

Los vecinos que tiene el R2 (Bogotá) son, el Sw0, el router de Cali y el router de Medellín.

```
BOGOTA#
BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
Sw0               Fas 0/0         141      S           2960      Fas 0/1
CALI              Ser 0/1/0       148      R           C2800     Ser 0/0/0
MEDELLIN          Ser 0/0/0       141      R           C2800     Ser 0/0/0
BOGOTA#
BOGOTA#
```

Los vecinos de R3 (Cali) son Sw2 y el router de Bogotá.

```
CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  Port ID
Sw2               Fas 0/0         148      S           2960      Fas 0/1
BOGOTA            Ser 0/0/0       157      R           C2800     Ser 0/1/0
CALI#
CALI#
```


1.7 PRUEBA DE CONECTIVIDAD USANDO EL COMANDO PING

El comando ping se utiliza para verificar la conectividad entre los dispositivos. Para su aplicación, se accede a la consola del dispositivo.

La prueba se realiza desde la PC1 en Medellín hacia la PC3 en Cali

```
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=9ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125
Reply from 192.168.1.67: bytes=32 time=24ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 24ms, Average = 9ms

C:\>
```

Prueba realizada desde la PC4 en Cali hacia el Servidor en Bogotá

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=5ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

1.8 CONFIGURACIÓN DE ENRUTAMIENTO

Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado y verificar si existe vecindad con los routers configurados con EIGRP

El Router de Medellín está conectado a la LAN de Medellín a través del puerto Fa0/0 del SW1 y al router de Bogotá por el puerto se0/0/0; ahora bien, si requiere conectarse al servidor por ejemplo, utiliza la ruta 192.168.1.98 puerto se0/0/0 del router de Bogotá y para conectarse a un equipo en Cali, igualmente utiliza la ruta 192.168.1.98 puerto se0/0/0 del router de Bogotá.

```
MEDELLIN#
MEDELLIN#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/27, 1 successors, FD is 20514560
    via 192.168.1.98 (20514560/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 28160
    via Connected, FastEthernet0/0
P 192.168.1.64/27, 1 successors, FD is 21026560
    via 192.168.1.98 (21026560/20514560), Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 20512000
    via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 21024000
    via 192.168.1.98 (21024000/20512000), Serial0/0/0
MEDELLIN#
```

El Router de Bogotá, está conectado al router de Medellín a través del puerto se0/0/0; al router de Cali por el puerto se0/1/0 y al Sw0 por el puerto Fa0/0 ahora bien, si requiere conectarse a la LAN de Medellín, utiliza la ruta 192.168.1.99 puerto se0/0/0 y para conectarse a un equipo en Cali, igualmente utiliza la ruta 192.168.1.98 puerto se0/1/0.

```
BOGOTA#
BOGOTA#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160
    via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 20514560
    via 192.168.1.99 (20514560/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 20514560
    via 192.168.1.131 (20514560/28160), Serial0/1/0
P 192.168.1.96/27, 1 successors, FD is 20512000
    via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 20512000
    via Connected, Serial0/1/0
BOGOTA#
```

El Router de Cali está conectado al router de Bogotá a través del puerto se0/0/0 y a la LAN por el puerto Fa0/0; ahora bien, si requiere conectarse al servidor por ejemplo, utiliza la ruta 192.168.1.130 puerto se0/0/0 y para conectarse a un equipo en Medellín, igualmente utiliza la ruta 192.168.1.130 puerto se0/0/0.

```
CALI#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.131)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/27, 1 successors, FD is 20514560
    via 192.168.1.130 (20514560/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 21026560
    via 192.168.1.130 (21026560/20514560), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 28160
    via Connected, FastEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 21024000
    via 192.168.1.130 (21024000/20512000), Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 20512000
    via Connected, Serial0/0/0
CALI#
```

1.9 COMPROBAR LAS TABLAS DE ENRUTAMIENTO

Con el comando `show ip route` se puede verificar el enrutamiento de cada router

```
MEDELLIN#
MEDELLIN#
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.98, 02:23:30, Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/21026560] via 192.168.1.98, 02:23:30, Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/21024000] via 192.168.1.98, 02:23:30, Serial0/0/0

MEDELLIN#
```

```

BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/20514560] via 192.168.1.99, 02:30:37, Serial0/0/0
D       192.168.1.64 [90/20514560] via 192.168.1.131, 02:30:39, Serial0/1/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/1/0

CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.130, 02:31:50, Serial0/0/0
D       192.168.1.32 [90/21026560] via 192.168.1.130, 02:31:48, Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/21024000] via 192.168.1.130, 02:31:48, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI#

```

Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Prueba de host de la red LAN del router de Cali hacia la red de Medellín.

La prueba se realiza desde PC4 hacia PC2

```

C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=11ms TTL=125
Reply from 192.168.1.36: bytes=32 time=3ms TTL=125
Reply from 192.168.1.36: bytes=32 time=3ms TTL=125
Reply from 192.168.1.36: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\>

```

Prueba de host de la red LAN del router de Medellín hacia el servidor en Bogotá. La prueba se ha efectuado desde PC1 en Medellín hacia el servidor en Bogotá

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=7ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms

C:\>
```

1.10 CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO

Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

Se realiza la configuración en cada uno de los routers:

```
MEDELLIN(config)# line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#
```

```
BOGOTA(config)# line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#
```

```
CALI(config)# line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#
```

El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor tendrá acceso a cualquier dispositivo en cualquier parte de la red. Para esta ACL, la configuración se realiza en el router de Bogotá.


```
BOGOTA(config)#access-list 3 permit host 192.168.1.10
BOGOTA(config)#access-list 3 deny any
BOGOTA(config)#interface fa0/0
BOGOTA(config-if)#ip access-group 3 in
```

Las estaciones de trabajo en las LAN de Medellín y Cali no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor. La configuración se realiza en el router de Cali y en el router de Medellín

En CALI

De LAN de Medellín hacia LAN de Cali

```
CALI(config)#access-list 1 deny 192.168.1.32 0.0.0.31
CALI(config)#access-list 1 permit any
CALI(config)#interface fa0/0
CALI(config-if)#ip access-group 1 out
```

En MEDELLIN

De LAN de Cali hacia LAN de Medellín

```
MEDELLIN (config)#access-list 2 deny 192.168.1.64 0.0.0.31
MEDELLIN (config)#access-list 2 permit any
MEDELLIN (config)#interface fa0/0
MEDELLIN (config-if)#ip access-group 2 out
```

1.11 COMPROBACIÓN DE LA RED INSTALADA

Comprobar que la configuración de las listas de acceso fue exitosa.

De LAN de Medellin a LAN de Cali

Se realiza la prueba desde el PC1 en Medellín hacia el PC4 en cali

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

De LAN de Cali a LAN de Medellín

Se realiza la prueba desde el PC3 en Cali hacia el PC2 en Medellín

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.99: Destination host unreachable.
Reply from 192.168.1.99: Destination host unreachable.
Reply from 192.168.1.99: Destination host unreachable.
Reply from 192.168.1.99: Destination host unreachable.

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

De LAN de Medellin a Servidor

Se realiza la prueba desde el PC1 en Medellín hacia el servidor en Bogotá

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

De LAN de Cali a Servidor

Se realiza la prueba desde el PC3 en Cali hacia el Servidor en Bogotá

```

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>

```

Desde WS1 hacia Medellín y Cali

Se realiza la prueba desde WS1 en Bogotá hacia el PC2 en Medellín y el PC4 en Cali.

```

C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Desde WS1 hacia el servidor

Se realiza la prueba desde el WS1 en Bogotá hacia el Servidor

```

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

1.12 TABLA DE CONDICIONES DE PRUEBA

Comprobar y completar la tabla de condiciones de prueba para confirmar el funcionamiento de la red.

| | ORIGEN | DESTINO | RESULTADO |
|---------------|--|-----------------|---|
| TELNET | Router MEDELLIN | Router CALI | MEDELLIN>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: CALI> |
| | WS1 | Router BOGOTA | C:\>telnet 192.168.1.1 Trying 192.168.1.1 ... % Connection timed out; remote host not responding C:\> |
| | Servidor | Router CALI | C:\>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: CALI> |
| | Servidor | Router MEDELLIN | C:\>telnet 192.168.1.99 Trying 192.168.1.99 ...Open User Access Verification Password: MEDELLIN> |
| TELNET | LAN del router MEDELLIN (Se utiliza el PC1) | Router CALI | C:\>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: CALI> |

| | | | |
|-------------|---|----------------------------|--|
| | LAN del Router CALI (Se utiliza el PC4) | Router CALI | C:\>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: CALI> |
| | LAN del router MEDELLIN (Se utiliza el PC1) | Router MEDELLIN | C:\>telnet 192.168.1.99 Trying 192.168.1.99 ...Open User Access Verification Password: MEDELLIN> |
| | LAN del Router CALI (Se utiliza el PC3) | Router MEDELLIN | C:\>telnet 192.168.1.99 Trying 192.168.1.99 ...Open User Access Verification Password: MEDELLIN> |
| PING | LAN del Router CALI | WS1 | Request timed out Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), |
| | LAN del Router MEDELLIN | WS1 | Request timed out Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), |
| | LAN del Router MEDELLIN | LAN del Router CALI | Destination host unreachable Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), |
| PING | LAN del Router CALI | Servidor | Reply from 192.168.1.10: bytes=32 time=1ms TTL=126 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), |
| | LAN del router MEDELLIN | Servidor | Reply from 192.168.1.10: bytes=32 time=1ms TTL=126 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), |
| | Servidor | LAN del Router MEDELLIN | Reply from 192.168.1.35: bytes=32 time=2ms TTL=126 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), |

| | | | |
|--|-----------------|-------------------------|--|
| | Servidor | LAN del Router CALI | Reply from 192.168.1.67: bytes=32 time=9ms TTL=126 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), |
| | Router CALI | LAN del Router MEDELLIN | CALI> CALI>ping 192.168.1.35 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/15 ms CALI> |
| | Router MEDELLIN | LAN del Router CALI | MEDELLIN>ping 192.168.1.67 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.67, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/14 ms MEDELLIN> |

2. ESCENARIO 2.

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyan puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

2.1 CONFIGURACION BASICA

Router Tunja

Ingreso al modo de configuración global

```
Router> configure terminal
```

```
Router(config) #
```

Asignación de un nombre al router

```
Router(config) # hostname TUNJA
```

```
TUNJA(config) #
```

Para evitar las búsquedas de DNS no deseada

```
TUNJA(config) # no ip domain-lookup
```

```
TUNJA(config) #
```

Para configurar un mensaje MOTD

```
TUNJA(config) # banner motd #
```

```
Enter Text message. End with the character `''`.
```

```
El acceso no autorizado está prohibido. #
```

```
TUNJA(config) #
```

Asegurar el acceso (EXEC privilegiado, EXEC de usuario y acceso remoto)

```
TUNJA(config) # enable secret class
```

```
TUNJA(config) #
```

```
TUNJA(config) # line console 0
```

```
TUNJA(config-line) # password cisco
```

```
TUNJA(config-line) # login
```

```
TUNJA(config-line) # exit
```

```
TUNJA(config) #
```

```
TUNJA(config) # line vty 0 4
```

```
TUNJA(config-line) # password cisco
```

```
TUNJA(config-line) # login
```

```
TUNJA(config-line) # exit
```

```
TUNJA(config) #
```

Configurar la encriptación de contraseñas

```
TUNJA(config) #
```

```
TUNJA(config)# service password-encryption
TUNJA(config)#
```

Un máximo de intentos para acceder a router

Si se falla en 3 intentos en menos de 1 minuto, el router se bloquea por 5 minutos (300 segundos).

```
TUNJA(config)#
TUNJA(config)# login block-for 300 attempts 3 within 60
TUNJA(config)#
```

Router Bucaramanga

Ingreso al modo de configuración global

```
Router> configure terminal
Router(config)#
```

Asignación de un nombre al router

```
Router(config)# hostname BUCARAMANGA
BUCARAMANGA(config)#
```

Para evitar las búsquedas de DNS no deseada

```
BUCARAMANGA(config)# no ip domain-lookup
BUCARAMANGA(config)#
```

Para configurar un mensaje MOTD

```
BUCARAMANGA(config)# banner motd #
Enter Text message. End with the character `'.
El acceso no autorizado está prohibido. #
BUCARAMANGA(config)#
```

Asegurar el acceso (EXEC privilegiado, EXEC de usuario y acceso remoto)

```
BUCARAMANGA(config)# enable secret class
BUCARAMANGA(config)#
BUCARAMANGA(config)# line console 0
BUCARAMANGA(config-line)# password cisco
BUCARAMANGA(config-line)# login
BUCARAMANGA(config-line)# exit
BUCARAMANGA(config)#
BUCARAMANGA(config)# line vty 0 4
BUCARAMANGA(config-line)# password cisco
BUCARAMANGA(config-line)# login
BUCARAMANGA(config-line)# exit
```

```
BUCARAMANGA (config) #
```

Configurar la encriptación de contraseñas

```
BUCARAMANGA (config) #  
BUCARAMANGA (config) # service password-encryption  
BUCARAMANGA (config) #
```

Un máximo de intentos para acceder a router

Si se falla en 3 intentos en menos de 1 minuto, el router se bloquea por 5 minutos (300 segundos).

```
BUCARAMANGA (config) #  
BUCARAMANGA (config) # login block-for 300 attempts 3 within 60  
BUCARAMANGA (config) #
```

Router Cundinamarca

Ingreso al modo de configuración global

```
Router> configure terminal  
Router (config) #
```

Asignación de un nombre al router

```
Router (config) # hostname CUNDINAMARCA  
CUNDINAMARCA (config) #
```

Para evitar las búsquedas de DNS no deseada

```
CUNDINAMARCA (config) # no ip domain-lookup  
CUNDINAMARCA (config) #
```

Para configurar un mensaje MOTD

```
CUNDINAMARCA (config) # banner motd #  
Enter Text message. End with the character `'''.  
El acceso no autorizado está prohibido. #  
CUNDINAMARCA (config) #
```

Asegurar el acceso (EXEC privilegiado, EXEC de usuario y acceso remoto)

```
CUNDINAMARCA (config) # enable secret class  
CUNDINAMARCA (config) #  
CUNDINAMARCA (config) # line console 0  
CUNDINAMARCA (config-line) # password cisco  
CUNDINAMARCA (config-line) # login  
CUNDINAMARCA (config-line) # exit  
CUNDINAMARCA (config) #  
CUNDINAMARCA (config) # line vty 0 4
```

```
CUNDINAMARCA(config-line)# password cisco
CUNDINAMARCA(config-line)# login
CUNDINAMARCA(config-line)# exit
CUNDINAMARCA(config)#
```

Configurar la encriptación de contraseñas

```
CUNDINAMARCA(config)#
CUNDINAMARCA(config)# service password-encryption
CUNDINAMARCA(config)#
```

Un máximo de intentos para acceder a router

Si se falla en 3 intentos en menos de 1 minuto, el router se bloquea por 5 minutos (300 segundos).

```
CUNDINAMARCA(config)#
CUNDINAMARCA(config)# login block-for 300 attempts 3 within 60
CUNDINAMARCA(config)#
```

2.2 ENRUTAMIENTO OSPF

Se configuran los puertos de los routers y se asignan direcciones IP

Router Tunja

```
TUNJA(config)#interface GigabitEthernet0/0
TUNJA(config-if)#ip address 172.31.3.129 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit
TUNJA(config)#interface GigabitEthernet0/1
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit
TUNJA(config)# interface Serial0/1/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit
TUNJA(config)# interface Serial0/1/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#clock rate 64000
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
```

Router Bucaramanga

```
BUCARAMANGA(config)# interface Serial0/1/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
```

```

CUNDINAMARCA(config-if)#clock rate 64000
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)# interface GigabitEthernet0/0
BUCARAMANGA(config-if)#ip address 172.31.3.1 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#

```

Router Cundinamarca

```

CUNDINAMARCA(config)#interface Serial0/1/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface GigabitEthernet0/0
CUNDINAMARCA(config-if)#ip address 172.31.3.65 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#

```

Se configura el OSPF en cada router

Router Bucaramanga

```

BUCARAMANGA(config)#
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.3.0 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#

```

Router Cundinamarca

```

CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#network 172.31.3.64 0.0.0.3 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#

```

Router Tunja

```

TUNJA(config)#
TUNJA(config)#router ospf 1
TUNJA(config-router)#network 172.31.3.128 0.0.0.3 area 0

```

```

TUNJA(config-router)#
TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#
01:52:03: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.3.1 on
Serial0/1/0 from LOADING to FULL, Loading Done

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#
01:52:22: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.3.65 on
Serial0/1/1 from LOADING to FULL, Loading Done

TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#
TUNJA(config-router)#

```

Se verifica la configuración de OSPF con el comando `show ip route ospf`

```

BUCARAMANGA#
BUCARAMANGA#sh ip route ospf
172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
O 172.31.2.36 [110/128] via 172.31.2.33, 00:14:22, Serial0/1/0
O 172.31.3.64 [110/129] via 172.31.2.33, 00:14:12, Serial0/1/0
O 172.31.3.128 [110/65] via 172.31.2.33, 00:14:41, Serial0/1/0
O 209.17.220.0 [110/65] via 172.31.2.33, 00:14:41, Serial0/1/0

```

```

BUCARAMANGA#

```

```

CUNDINAMARCA#
CUNDINAMARCA#sh ip route ospf
172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
O 172.31.2.32 [110/128] via 172.31.2.37, 00:16:43, Serial0/1/0
O 172.31.3.0 [110/129] via 172.31.2.37, 00:16:43, Serial0/1/0
O 172.31.3.128 [110/65] via 172.31.2.37, 00:16:43, Serial0/1/0
O 209.17.220.0 [110/65] via 172.31.2.37, 00:16:43, Serial0/1/0

```

```

CUNDINAMARCA#

```

```

TUNJA#
TUNJA#sh ip route ospf
172.31.0.0/16 is variably subnetted, 8 subnets, 2 masks
O 172.31.3.0 [110/65] via 172.31.2.34, 00:13:40, Serial0/1/0
O 172.31.3.64 [110/65] via 172.31.2.38, 00:13:20, Serial0/1/1

```


TUNJA#

2.3 VLAN Y DHCP EQUIPOS DE BUCARAMANGA Y CUNDINAMARCA

Bucaramanga

Se asignan las subinterfaces en el router

```
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#
```

Se configura el dhcp

```
BUCARAMANGA(config)#
BUCARAMANGA(config)#ip dhcp pool vlan10
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#dns-server 209.17.220.100
BUCARAMANGA(dhcp-config)#exit
BUCARAMANGA(config)#
BUCARAMANGA(config)#ip dhcp pool vlan30
BUCARAMANGA(dhcp-config)#network 172.31.0.64 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.65
BUCARAMANGA(dhcp-config)#dns-server 209.17.220.100
BUCARAMANGA(dhcp-config)#end
BUCARAMANGA(config)#ip dhcp excluded-address 172.31.0.65
BUCARAMANGA(config)#ip dhcp excluded-address 172.31.0.1
BUCARAMANGA(config)#
```

Se crean las vlan y se configura el puerto troncal y los puertos de acceso en el switch

```
Sw-Bucaramanga(config)#
```

```

Sw-Bucaramanga(config)#int f0/24
Sw-Bucaramanga(config-if)#switchport mode trunk
Sw-Bucaramanga(config-if)#
Sw-Bucaramanga(config-if)#exit
Sw-Bucaramanga(config)#
Sw-Bucaramanga(config)#vlan 10
Sw-Bucaramanga(config-vlan)#name vlan10
Sw-Bucaramanga(config-vlan)#exit
Sw-Bucaramanga(config)#vlan 30
Sw-Bucaramanga(config-vlan)#name vlan30
Sw-Bucaramanga(config-vlan)#exit
Sw-Bucaramanga(config)#
Sw-Bucaramanga(config)#int fa0/1
Sw-Bucaramanga(config-if)#switchport mode access
Sw-Bucaramanga(config-if)#switchport access vlan 10
Sw-Bucaramanga(config-if)#exit
Sw-Bucaramanga(config)#
Sw-Bucaramanga(config)#int fa0/2
Sw-Bucaramanga(config-if)#switchport mode access
Sw-Bucaramanga(config-if)#switchport access vlan 30
Sw-Bucaramanga(config-if)#exit
Sw-Bucaramanga(config)#

```

Cundinamarca

```

CUNDINAMARCA(config)#
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#int g0/0.30
CUNDINAMARCA(config-subif)#
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#int g0/0.88
CUNDINAMARCA(config-subif)#
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#

```

Se configura el dhcp

```
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#ip dhcp pool vlan20
CUNDINAMARCA(dhcp-config)#network 172.31.1.64 255.255.255.192
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.65
CUNDINAMARCA(dhcp-config)#dns-server 209.17.220.100
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#ip dhcp pool vlan30
CUNDINAMARCA(dhcp-config)#network 172.31.1.0 255.255.255.192
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.1
CUNDINAMARCA(dhcp-config)#dns-server 209.17.220.100
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#ip dhcp pool vlan88
CUNDINAMARCA(dhcp-config)#network 172.31.2.24 255.255.255.248
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.25
CUNDINAMARCA(dhcp-config)#dns-server 209.17.220.100
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#ip dhcp excluded-address 172.31.1.65
CUNDINAMARCA(config)#ip dhcp excluded-address 172.31.1.1
CUNDINAMARCA(config)#ip dhcp excluded-address 172.31.2.25
CUNDINAMARCA(config)#
```

Se crean las vlan y se configura el puerto troncal y los puertos de acceso en el switch

```
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#int f0/24
Sw-Cundinamarca(config-if)#switchport mode trunk
Sw-Cundinamarca(config-if)#
Sw-Cundinamarca(config-if)#exit
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#vlan 20
Sw-Cundinamarca(config-vlan)#name vlan20
Sw-Cundinamarca(config-vlan)#exit
Sw-Cundinamarca(config)#vlan 30
Sw-Cundinamarca(config-vlan)#name vlan30
Sw-Cundinamarca(config-vlan)#exit
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#vlan 88
Sw-Cundinamarca(config-vlan)#name vlan88
```

```

Sw-Cundinamarca(config-vlan)#exit
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#int fa0/5
Sw-Cundinamarca(config-if)#switchport mode access
Sw-Cundinamarca(config-if)#switchport access vlan 20
Sw-Cundinamarca(config-if)#exit
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#int fa0/6
Sw-Cundinamarca(config-if)#switchport mode access
Sw-Cundinamarca(config-if)#switchport access vlan 30
Sw-Cundinamarca(config-if)#exit
Sw-Cundinamarca(config)#
Sw-Cundinamarca(config)#int fa0/7
Sw-Cundinamarca(config-if)#switchport mode access
Sw-Cundinamarca(config-if)#switchport access vlan 88
Sw-Cundinamarca(config-if)#exit
Sw-Cundinamarca(config)#exit
Sw-Cundinamarca#

```

2.4 ALMACENAMIENTO EN SERVIDOR TFTP

Para guardar el archivo IOS del router, se debe introducir el comando **dir flash** en la consola para establecer cuál es el archivo a guardar.

Router Bucaramanga

```

BUCARAMANGA#dir flash
Directory of flash0:/

 3 -rw- 33591768 <no date> c1900-universalk9-mz.SPA.151-4.M4.bin
 2 -rw- 28282 <no date> sigdef-category.xml
 1 -rw- 227537 <no date> sigdef-default.xml

255744000 bytes total (221896413 bytes free)
BUCARAMANGA#

```

Seguidamente se ejecuta el comando que guardará el archivo en el servidor TFTP indicándole el nombre del archivo que se va a copiar y el nombre del archivo con el cual se quiere guardar los datos (Para este caso es Router-Bucaramanga

```

BUCARAMANGA#

```

```
BUCARAMANGA#copy flash: tftp
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.31.2.27
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?
Router-Bucaramanga
```

```
Writing c1900-universalk9-mz.SPA.151-
4.M4.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]
```

```
33591768 bytes copied in 7.469 secs (472218 bytes/sec)
BUCARAMANGA#
```

Router Cundinamarca

```
CUNDINAMARCA#
CUNDINAMARCA#dir flash
Directory of flash0:/

 3 -rw- 33591768 <no date> c1900-universalk9-mz.SPA.151-4.M4.bin
 2 -rw- 28282 <no date> sigdef-category.xml
 1 -rw- 227537 <no date> sigdef-default.xml

255744000 bytes total (221896413 bytes free)
CUNDINAMARCA#
```

Ahora se realiza la copia del archivo

```
CUNDINAMARCA#
CUNDINAMARCA#copy flash
CUNDINAMARCA#copy flash: tftp
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.31.2.27
```



```

TUNJA(config)#ip dhcp excluded-address 172.31.0.193
TUNJA(config)#ip dhcp excluded-address 172.31.0.129
TUNJA(config)#
Sw-Tunja(config-if)#
Sw-Tunja(config-if)#exit
Sw-Tunja(config)#
Sw-Tunja(config)#vlan 20
Sw-Tunja(config-vlan)#name vlan20
Sw-Tunja(config-vlan)#exit
Sw-Tunja(config)#vlan 30
Sw-Tunja(config-vlan)#name vlan30
Sw-Tunja(config-vlan)#exit
Sw-Tunja(config)#int f0/3
Sw-Tunja(config-if)#switchport mode access
Sw-Tunja(config-if)#switchport access vlan 20
Sw-Tunja(config-if)#exit
Sw-Tunja(config)#int f0/4
Sw-Tunja(config-if)#switchport mode access
Sw-Tunja(config-if)#switchport access vlan 30
Sw-Tunja(config-if)#exit
Sw-Tunja(config)#
Sw-Tunja(config)#

```

2.6 LISTAS DE CONTROL DE ACCESO

Los hosts de VLAN 10 en Bucaramanga, acceden a la red de Cundinamarca (VLAN 20) y Tunja(VLAN 20), no a internet

En el router de Tunja se restringe el acceso a internet de la VLAN 10 de Bucaramanga

```

TUNJA(config)#
TUNJA(config)#access-list 1 deny 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 1 permit any
TUNJA(config)#int g0/1
TUNJA(config-if)#ip access-group 1 out
TUNJA(config-if)#
TUNJA(config-if)#

```

En el router de Cundinamarca se restringe el acceso a la VLAN 30 de la VLAN 10 de Bucaramanga


```

CUNDINAMARCA(config)#
CUNDINAMARCA(config)#access-list 2 deny 172.31.0.0 0.0.0.63
CUNDINAMARCA(config)#access-list 2 permit any
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#ip access-group 2 out
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#

```

En el router de Tunja se restringe el acceso a la VLAN 30 de la VLAN 10 de Bucaramanga

```

TUNJA#
TUNJA(config)#access-list 3 deny 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 3 permit any
TUNJA(config)#int g0/0.30
TUNJA(config-subif)#ip access-group 3 out
TUNJA(config-subif)#exit
TUNJA(config)#

```

Los hosts de VLAN 20 en Cundinamarca no acceden a internet, sólo a la red interna de Tunja

En el router de Tunja se restringe el acceso a internet de la VLAN 20 de Cundinamarca.

```

TUNJA(config)#
TUNJA(config)#access-list 3 deny 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 3 permit any
TUNJA(config)#int g0/0.30
TUNJA(config-subif)#ip access-group 3 out
TUNJA(config-subif)#exit
TUNJA(config)#
TUNJA(config)#access-list 4 deny 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 4 permit any
TUNJA(config)#int g0/1
TUNJA(config-if)#ip access-group 4 out
TUNJA(config-if)#

```

En el router de Bucaramanga se restringe el acceso a internet de la VLAN 20 de Cundinamarca para las VLAN 10 y 30

```

BUCARAMANGA(config)#
BUCARAMANGA(config)#access-list 5 deny 172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 5 permit any

```

```

BUCARAMANGA(config)#
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip access-group 5 out
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#ip access-group 5 out
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#
BUCARAMANGA(config)#

```

Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga

En el router de Cundinamarca se restringe el acceso a la VLAN 30 de la VLAN 20 Tunja

```

CUNDINAMARCA(config)#
CUNDINAMARCA(config)#access-list 6 deny 172.31.0.128 0.0.0.63
CUNDINAMARCA(config)#access-list 6 permit any
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#int g0/0.30
CUNDINAMARCA(config-subif)#ip access-group 6 out
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#

```

En el router de Cundinamarca se restringe el acceso a la VLAN 30 de la VLAN 20 de Tunja

```

BUCARAMANGA(config)#
BUCARAMANGA(config)#access-list 7 deny 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#access-list 7 permit any
BUCARAMANGA(config)#
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#ip access-group 7 out
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#

```

3. CONCLUSIONES

Después de realizado este documento se puede concluir que

- En la configuración del enrutamiento OSPF en un router, deben participar todos los puertos que estén habilitados y funcionando en el mismo.
- El servicio DHCP se configura utilizando subinterfaces en el router y enlaces troncales en el switch.
- Las ACL se configuran en el puerto de destino del router asignando un número a cada una para diferenciarlas dentro de la red.

4. REFERENCIAS BIBLIOGRÁFICAS

- Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M. (2002). *Redes de computadores para ingenieros en informática. Capítulo 11: Protocolo de nivel de red IP*. Recuperado de <http://search.ebscohost.com/bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=318062&lang=es&site=eds-live&scope=site>
- Boronat, S. F., & Montagud, C. M. (2013). *Direccionamiento e interconexión de redes basada en tcp/ip: ipv4/ipv6, dhcp, nat, encaminamiento rip y ospf*. Recuperado de: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co>
- Carceller, C. R., Campos, S. C., & García, M. C. J. (2013). *Servicios en red Unidad 3: Servicio de configuración dinámica de sistemas (DHCP)*. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co>
- Colobran, H. M., Arqués, S. J. M., & Marco, G. E. (2008). *Administración de sistemas operativos en red*. Recuperado de: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co>
- Molina Robles, Francisco José & Ortega, Eduardo Polo. (2014). *Servicios en Red*. RA-MA Editorial.
- Rashid, N. bin A., Othman, M. Z., Johan, R., & Sidek, S. F. bin H. (2019). Cisco Packet Tracer Simulation as Effective Pedagogy in Computer Networking Course. *International Journal of Interactive Mobile Technologies*. Recuperado de: <https://doi-org.bibliotecavirtual.unad.edu.co/10.3991/ijim.v13i10.11283>
- Santos González, Manuel. (2014). *Sistemas Telemáticos*. Madrid. RA-MA Editorial.